U. S. Department of Energy

Information Systems Security Incident Report

Date, time, and place (site) incident occurred_____Date of report_____
Person completing this report_____
Telephone Number_____e-mail_____

Type of incident:

- ❑ Intrusion attempt (successful)
- ❑ Intrusion attempt (not successful)
- ❑ Malicious code (virus, trojan horse, etc.)
- ❑ Unauthorized disclosure of information
- ❑ Denial of service attack
- ❑ Misuse
- ❑ Other_____

Loss associated with the incident:

Time: ❑ < 1 hour ❑ 1-24 hours ❑ 24-48 hours ❑ 2-5 days ❑ > 5 days
Cost: ❑ < $10,000 ❑ $10,000 - $50,000 ❑ > $50,000
❑ Loss, or potential loss, of reputation

Ranking of incident:

❑ Significant ❑ Important ❑ Routine
Justification for ranking _____
_____
Was this incident reportable under ORPS? ❑ Yes ❑ No

Classification and sensitivity levels of system/information involved in incident. Check all that apply:

System:

- ❑ Unclassified
  - ❑ Non-sensitive
  - ❑ Sensitive
- ❑ Classified
  - ❑ Confidential
  - ❑ Secret
  - ❑ Top Secret
  - ❑ NSI (National Security Information)
  - ❑ RD (Restricted Data)
  - ❑ SCI (Sensitive Compartmented Information)

Data/Information:

- ❑ Unclassified
  - ❑ Non-sensitive
  - ❑ Sensitive
    - ❑ UCNI ❑ NNPI ❑ EXPORT/IMPORT
    - ❑ OUO ❑ CRADA ❑ Business Proprietary
    - ❑ Medical ❑ Personnel ❑ Financial
    - ❑ Proprietary software ❑ Password file(s)
    - ❑ Other_____
- ❑ Classified
  - ❑ Confidential
  - ❑ Secret
  - ❑ Top Secret
  - ❑ NSI (National Security Information)
  - ❑ RD (Restricted Data)
  - ❑ SCI (Sensitive Compartmented Information)

What system platform was involved?_____

What was the damage to the affected data?

❑ Stolen ❑ Modified ❑ Deleted ❑ Encrypted ❑ Copied
❑ None ❑ Unknown ❑ Other_____

What was the damage to the affected network(s)?

❑ Local access interrupted ❑ Internet access interrupted ❑ None
❑ Other_____

What was the damage to the affected system?

❑ Service Interrupted
- ❑ User Access ❑ E-mail server ❑ Web-server
- ❑ Ftp ❑ Other_____

❑ Other_____

How was the incident discovered?

❑ A user ❑ An incident response team ❑ Another Site
❑ Audit logs ❑ Noticed unusual activity/behavior ❑ Other_____

Was the originating source of the incident located? ❑ Yes ❑ No

If yes, what was the source of the incident?

For malicious code:
- ❑ Diskette ❑ Downloaded file ❑ Attachment
- ❑ Obtained while on foreign travel ❑ System used anti-virus software

For an intrusion attempt:
- ❑ Insider
- ❑ Outsider
  - ❑ .gov ❑ .mil ❑ .edu ❑ .org ❑ .com
- ❑ Non-US. If Non-US what country_____

For a denial-of-service attack:
- ❑ Insider
- ❑ Outsider
  - ❑ .gov ❑ .mil ❑ .edu ❑ .org ❑ .com
- ❑ Non-US. If Non-US what country_____

Was law enforcement contacted regarding this incident? ❑ Yes ❑ No

If yes: Was the intruder identified? ❑ Yes ❑ No
Was the intruder prosecuted? ❑ Yes ❑ No

Was CIAC contacted regarding this incident?❑ Yes ❑ No

If yes: CIAC incident number_____
Date incident was opened_____ Date incident was closed_____